Aplikasi *Authentication* dan *Digital Signature Scheme* dengan Metode Schnoor untuk Implementasi Data Penggajian

Prawido Utomo[1], Ade Setiawan[2]
[1]Dosen STMIK Bina Sarana Global, [2]Mahasiswa STMIK Bina Sarana Global
Email : [1]prawidoutomo@stmikglobal.ac.id, [2]ade.setiawan20@yahoo.com

***Abstrak*— Data atau informasi merupakan salah satu unsur penting dalam banyak bidang kehidupan. Dengan perkembangan teknologi komputer, banyak orang yang mampu mengutak-atik data meskipun telah tersimpan rapi. keamanan tentang data penggajian di PT. Sandipala Arthaputra juga sangat penting. Saat ini, data penggajian pada Sandipala Arthaputra diletakkan pada folder berbagi itu memungkinkan data yang akan dimanipulasi oleh orang yang tidak bertanggung jawab. Untuk mengatasi ini, diperlukan Perangkat Lunak *Authentication* dan *Digital Signature Scheme* dengan metode Schnoor untuk implementasi dalam data penggajian. Dalam Penelitian ini, peneliti melakukan Observasi dan Studi Pustaka sebagai metodologi penelitian digunakan untuk mendapatkan keterangan dan penjelasan tentang situasi dan alur objek penelitian berdasarkan fakta. Dann juga untuk pengumpulan data. UML (*Unified Modelling Language*) digunakan untuk menjabarkan alur sistem sehingga mudah dipahami sehingga aplikasi bisa digunakan dengan maksimal dalam meningkatkan keamanan data yang bersifat confidential. Untuk implementasi menggunakan Aplikasi VB 6 dan MySQL. Kesimpulan dari penelitian dan perancangan Perangkat Lunak *Authentication* dan *Digital Signature Scheme* dengan metode *Schnoor* untuk implementasi dalam data penggajian ini untuk meningkatkan keamanan data penggajian pada PT. Sandipala Arthaputra.**

***Kata kunci*— *Autentication* dan *digital signature scheme, schnoor application*, VB6, MySQL.**

I. PENDAHULUAN

Data atau informasi merupakan salah satu elemen yang memegang peranan yang sangat besar dalam berbagai bidang kehidupan. Dengan semakin berkembangnya teknologi komputer, semakin banyak orang yang sanggup mengutak-atik data walaupun telah disimpan dengan rapi. Untuk mencegah terjadinya pencurian data oleh pihak-pihak yang tidak berhak atas data tersebut, maka dikembangkanlah berbagai teknik pengamanan data. Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu data atau informasi. Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan suatu pesan atau
data. Dalam hal ini pesan akan dienkripsi sehingga pesan tersebut tidak dapat dipahami lagi maknanya. Pesan yang sudah dienkripsi harus didekripsikan supaya pesan tersebut kembali seperti semula. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

PT. Sandipala Arthaputra adalah salah satu perusahaan percetakan yang bergerak dibidang Smart Card dan Security Printing yang mana pada akhir periode akuntansi (bulan) melakukan proses penggajian kepada para karyawannya dan membuat laporan gaji sebagai pertanggungjawaban kepada pimpinan perusahaan. Proses pencatatan dan perhitungan gaji yang diterapkan oleh perusahaan masih sangat sederhana dimana tingkat keamanan data nya masih sangat minim sehingga memungkinkan data penggajian bisa dirubah oleh pihak-pihak yang tidak bertanggung jawab. Oleh sebab itu perusahaan ini sebenarnya membutuhkan suatu sistem yang bisa melindungi keamanan data penggajian nya.

Berdasarkan uraian di atas, penulis bermaksud untuk mengambil penelitian dengan judul "Perangkat Lunak *Authentication* dan *Digital Signature Scheme* dengan metode Schnoor Untuk Impelementasi Pada Data Penggajian di PT. Sandipala Arthaputra".

Adapun permasalahan yang dihadapi oleh PT. Sandipala Arthaputra adalah Tingkat keamanan data penggajian yang masih sangat rendah dan belum adanya otentikasi data sehingga memungkinkan data dirubah oleh pihak yang tidak bertanggung jawab.

Karena keterbatasan waktu dan mengingat banyaknya permasalahan yang dihadapi oleh perusahaan maka penulis melakukan pembatasan masalah. Adapun batasan masalah ini adalah:

1. Perancangan Perangkat Lunak *Authentication* dan *Digital Signature Scheme* dengan metode *Schnoor* Untuk Impelementasi Pada Data Penggajian di PT. Sandipala Arthaputra.
2. Format database menggunakan MySql.
3. Perancangan program menggunakan bahasa pemrograman Microsoft Visual Basic 6.0.
4. Laporan disusun dengan menggunakan *Seagate Crystal Report* 8.5.

Adapun tujuan dari penelitian ini diantaranya yaitu:

a. Untuk mengetahui apa dan bagaimana sistem pengolahan data yang dilakukan oleh PT. Sandipala Arthaputra.
b. Dapat mengetahui kendala dan solusi dari sistem berjalan yang dilakukan oleh PT. Sandipala Arthaputra.
c. Merancang suatu Perangkat Lunak *Authentication* dan *Digital Signature Scheme* dengan metode *Schnoor* Untuk Impelementasi Pada Data Penggajian di PT. Sandipala Arthaputra.

II. METODOLOGI PENELITIAN

Dalam penyusunan penelitian ini saya menggunakan beberapa metode yaitu:

1. Metode Observasi Penulis Melakukan Observasi yaitu dengan cara mendatangi langsung ke PT.Sandipala Arthaputra dan melakukan pengamatan terhadap sistem keamanan data yang sudah berjalan dan melakukan pertanyaan terhadap user mengenai system keamanan data yang digunakan.
2. Metode Kepustakaan Metode Kepustakaan yaitu pengumpulan data-data dengan cara mempelajari berbagai bentuk bahan-bahan tertulis seperti buku-buku penunjang kajian, majalah, catatan-catatan maupun referensi lain yang bersifat tertulis.

Menurut Al Bahra bin Ladjamudin (2011:3) Perangkat lunak adalah objek tertentu yang dapat dijalankan seperti kode sumber, kode objek atau sebuah program yang lengkap.

Menurut Jogiyanto (2010:113) tentang Program Aplikasi adalah sederetan kode yang digunakan untuk mengatur komputer agar dapat melakukan pekerjaan sesuai dengan keinginan dari permasalahan pengguna.

Otentikasi (*authentication*) merupakan sebuah istilah yang digunakan dalam pengertian yang luas. Secara tersirat kata tersebut mempunyai arti lebih dari sekedar menyampaikan ide yaitu bahwa alat tersebut telah menyediakan jaminan bahwa informasi tidak dimanipulasi oleh pihak yang tidak mempunyai wewenang. Otentikasi bersifat spesifik dalam topik keamanan yang berusaha dicapai. Contohnya meliputi pengendalian akses, otentikasi entity, otentikasi pesan, integritas data, *non-repudiation*, dan otentikasi kunci.

Digital Signature adalah suatu mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tanda tangan tersebut menjamin integritas dan sumber dari sebuah pesan. Penandatanganan digital terhadap suatu dokumen adalah sidik jari dari dokumen tersebut beserta *timestamp*-nya dienkripsi dengan menggunakan kunci privat pihak yang menandatangani. Tanda tangan digital memanfaatkan fungsi hash satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Keabsahan tanda tangan digital itu dapat diperiksa oleh pihak yang menerima pesan.

Sifat yang diinginkan dari tanda tangan digital diantaranya adalah :

a. Tanda tangan itu asli (otentik), tidak mudah ditulis / ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia pernah menandatanganinya.
b. Tanda tangan itu hanya sah untuk dokumen (pesan) itu saja. Tanda tangan itu tidak bisa dipindahkan dari suatu dokumen ke dokumen lainnya. Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
c. Tanda tangan itu dapat diperiksa dengan mudah.
d. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
e. Tanda tangan itu juga sah untuk *copy* dari dokumen yang sama persis.

Claus Schnorr Authentication dan *Digital Signature scheme* mengambil sekuritas dari permasalahan menghitung logaritma diskrit. Skema ini juga menggunakan bilangan prima dan perpangkatan modulo dalam proses pembentukan kuncinya. Tingkat kesulitan untuk memecahkan algoritma ini adalah sekitar 2t, dimana nilai t ini dapat ditentukan sendiri.

Implementasi menurut Mazmanian dan Sebastier merupakan pelaksanaan kebijakan dasar berbentuk undang-undang juga berbentuk perintah atau keputusan-keputusan yang penting atau seperti keputusan badan peradilan. Proses implementasi ini berlangsung setelah melalui sejumlah tahapan tertentu seperti tahapan pengesahan undang-undang, kemudian output kebijakan dalam bentuk pelaksanaan keputusan dan seterusnya sampai perbaikan kebijakan yang bersangkutan. Menurut Mulyadi(2010,p.407), gaji merupakan pembayaran atas penyerahan jasa yang dilakukan olehkaryawan yang mempunyai jenjang jabatan seperti manajer. Sedangkan upah umumnya merupakan pembayaran jasa yang dilakukan oleh karyawan pelaksana (buruh). Umumnya gaji dibayarkan secara tetap perbulan, sedangkan upah dibayarkan berdasarkan hasil kerja atau jumlah satuan produk yang dihasilkan karyawan. Menurut Rosa A. S. dan M. Salahuddin (2013 : 133) *Unified Modeling Language* adalah standar bahasa yang banyak digunakan didunia industi untuk mendefinisikan requirement, membuat analisis dan desain, serta menggambarkan arsitektur dalam pemograman berorientasi objek.

Menurut Rosa A. S. dan M. Salahuddin (2013 : 141) pengertian Class Diagram adalah diagram untuk menggambarkan struktur system dari segi pendefinisian kelas – kelas yang akan dibuat untuk membangun sistem.

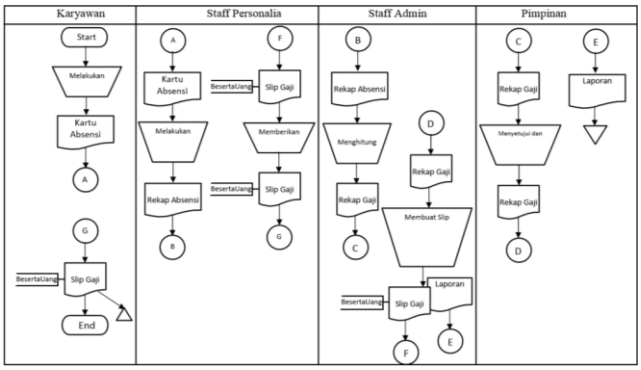
Menurut Rosa A. S. dan M. Salahuddin (2013 : 147) pengertian *Object diagram* menggambarkan struktur system dari segi penanaman objek dan jalannya objek dalam sistem.

Menurut Rosa A. S. dan M. Salahuddin (2013 : 155) pengertian Use Case diagram adalah merupakan pemodelan untuk kelakuan (Behavior) system informasi yang akan dibuat".

Flow Chart adalah bagian yang menunjukkan alir dalam program atau prosedur sistem secara logika. Bagan alir ini digunakan untuk alat bantu komunikasi dan dokumentasi.

III. ANALISA SISTEM YANG BERJALAN

A. *Flowcchart Sistem Berjalan*



Gambar 1. *Flowchart* Sistem Berjalan

IV. HASIL DAN BAHASAN

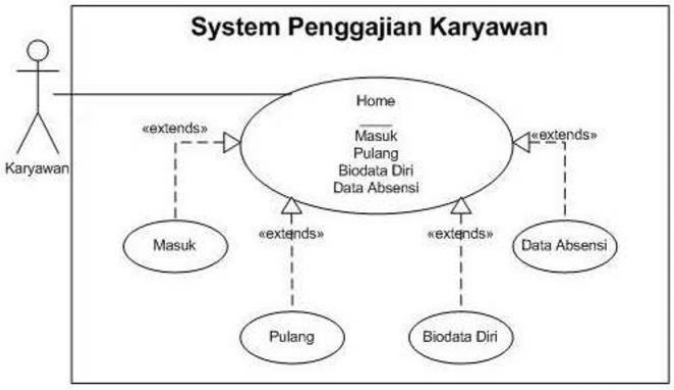
Setelah melihat sistem yang ada dan data yang didapat dari wawancara yang telah dilakukan maka didapatkan beberapa masalah yang dihadapi PT. Sandipala Arthaputra Sebagai Berikut :

1. Keamanan Data Belum Terjamin Data yang disimpan itu diletakan dalam folder sharing sehingga kemungkinan besar dapat dilihat oleh setiap karyawan karna security masih kurang. Seluruh data dapat dilihat maupun diubah sewaktu-waktu dengan kesempatan yang sangat besar.Sehingga integritas dan keakuratan data kurang terjamin.
2. Otentikasi data yang Belum Akurat Absensi manual yang masih menggunakan kartu absensi memungkinkan karyawan untuk bisa memanipulasi data kehadiran.

Berdasarkan analisa terhadap sistem yang berjalan, dapat diambil kesimpulan bahwa perlu diadakan pengembangan sistem atas kekurangan dan kebutuhan sistem dengan melakukan analisa terhadap alternatif pemecahan masalah antara lain :

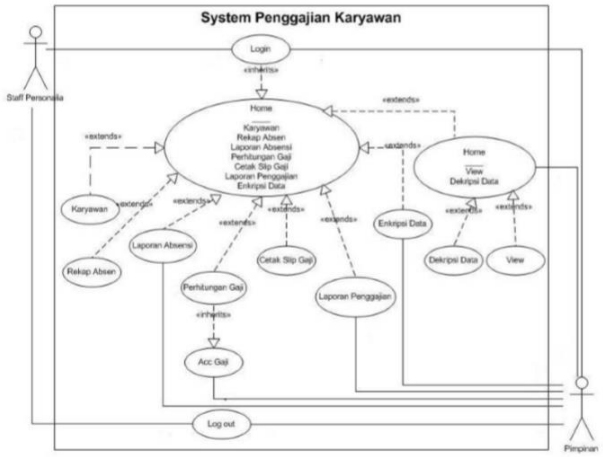
1. Membangun sistem yang dibutuhkan oleh user dengan menggunakan aplikasi berbasis visual karena aplikasi yang berbasis visual sudah familiar dikalangan instansi masyarakat.
2. Membangun suatu aplikasi sistem security yang berbasiskan Desktop yang memungkinkan user dapat menggunakan data secara bersama-sama di dalam waktu yang sama tetapi juga mengutamakan keamanan dan otentikasi data.

A. *Use case diagram karyawan Usulan*



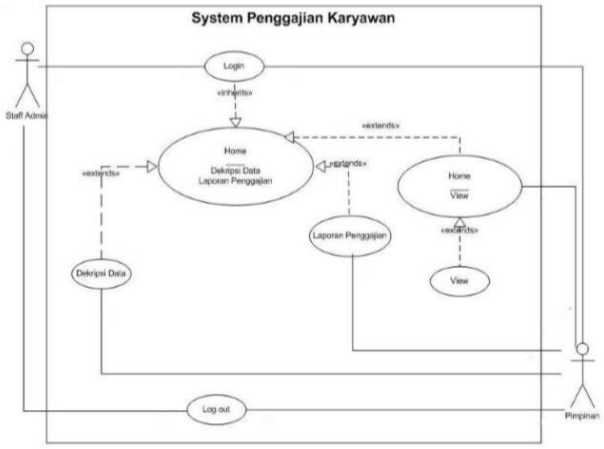
Gambar 2. *Use Case Diagram* Karyawan Usulan

B. *Use case diagram Staff Personalia Usulan*



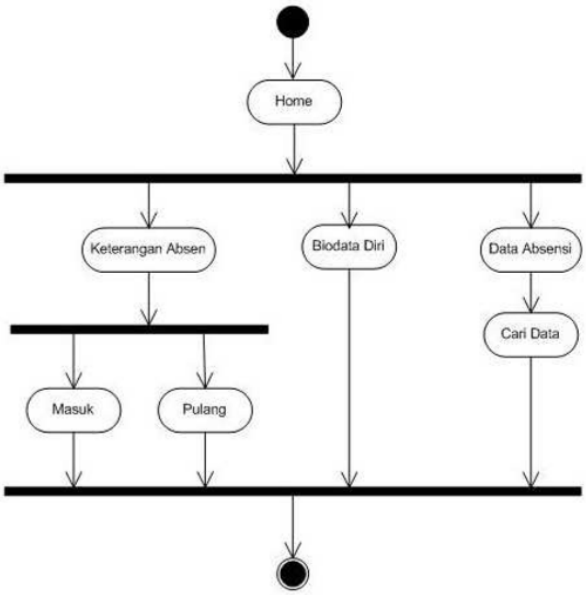
Gambar 3. *Use Case Diagram* Staff Personalia Usulan

C. *Use Case Diagram Staff Admin Usulan*



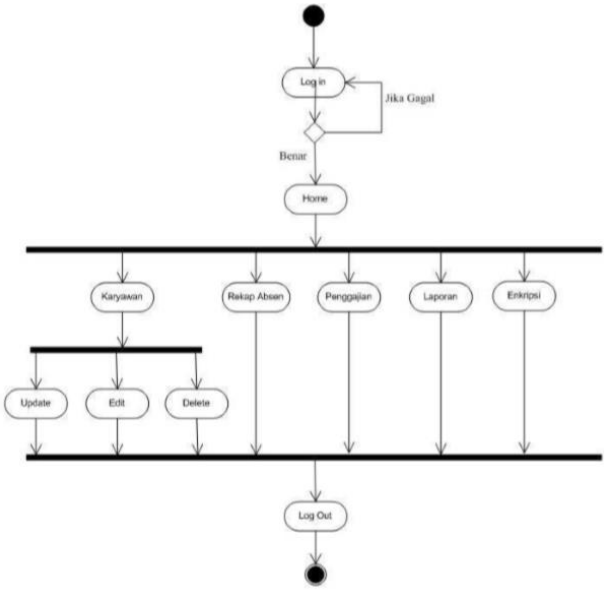
Gambar 4. *Use Case Diagram* pada Staff Admin Usulan

D. Activity diagram Karyawan Usulan



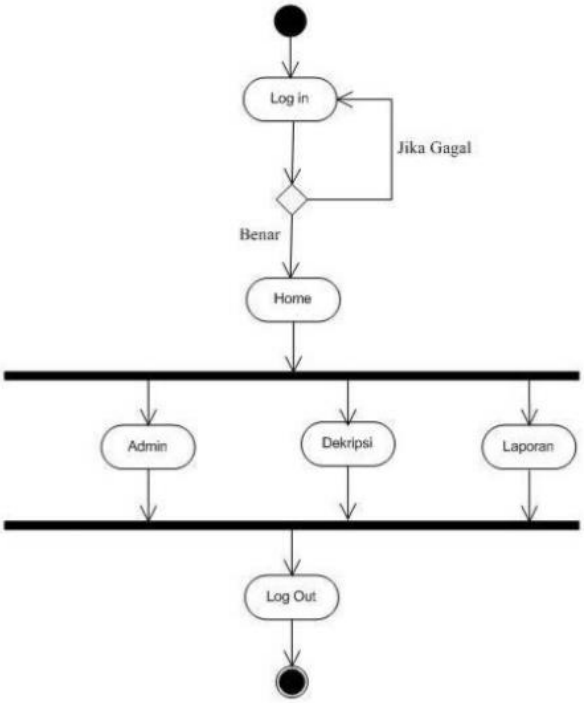
Gambar 5. *Activity Diagram* Karyawan Usulan

E. Activity diagram Staff Personalia Usulan



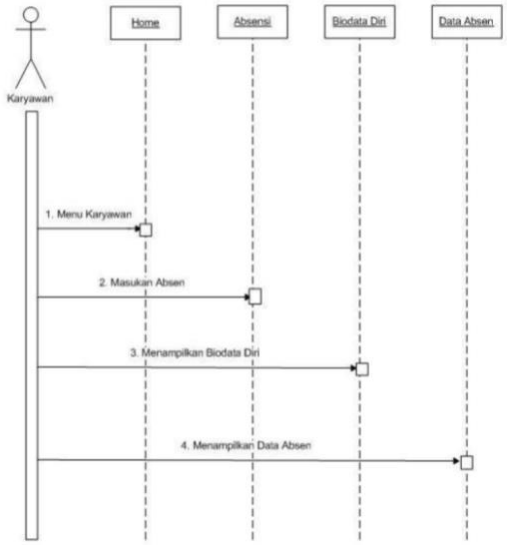
Gambar 6. *Activity Diagram* Staff Personalia Usulan

F. Activity diagram Staff Admin Usulan



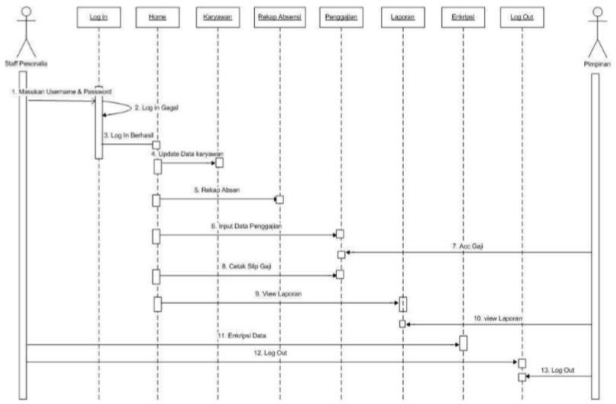
Gambar 7. *Activity Diagram* Staff Admin Usulan

G. Sequence diagram Karyawan Usulan



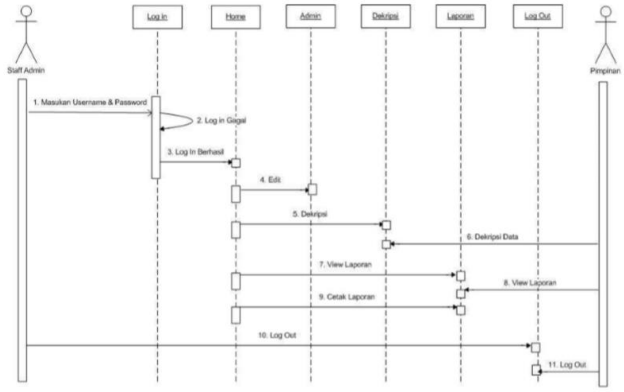
Gambar 8. *Sequence Diagram* Karyawan Usulan

H. Sequence diagram Staff Personalia Usulan



Gambar 9. *Sequence Diagram* Staff Personalia Usulan

I. Sequence diagram Staff Admin Usulan



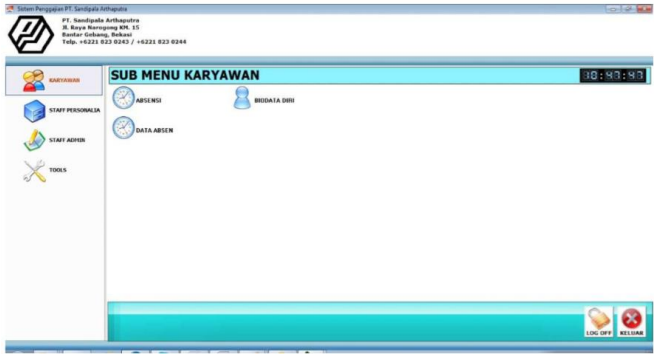
Gambar 10. *Sequence Diagram* Staff admin Usulan

Perancangan masukan adalah form pengisian data-data diinput kemudian diproses. Usulan perancangan masukan ini adalah sebagai berikut:

1. Nama Form : Form Login
   Fungsi : Untuk Login User agar mendapatkan hak akses

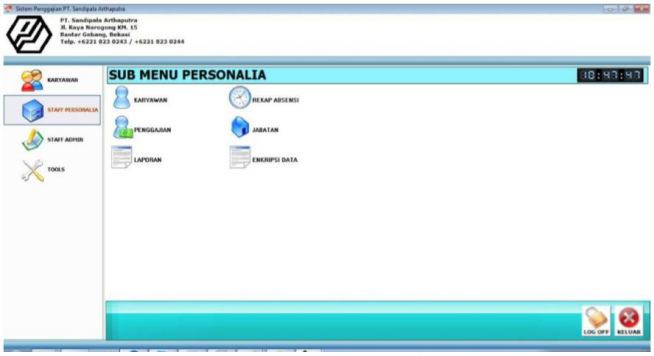
Gambar 11. *Form Login*

2. Nama Form : Menu Karyawan
   Fungsi : Tampilan Awal karyawan setelah login



Gambar 12. Tampilan menu Karyawan

3. Nama Form : Menu Staff Personalia
   Fungsi : Tampilan Awal Staff Personalia Setelah Login

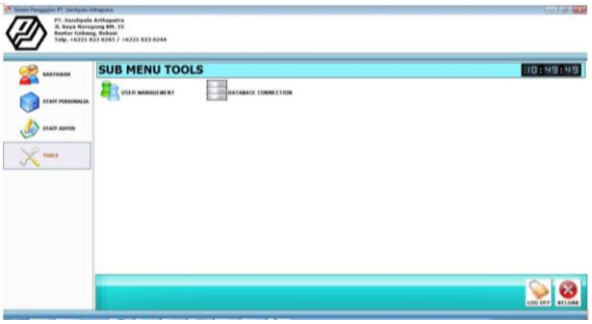


Gambar 13. Tampilan Menu Staff Personalia

4. Nama Form : Menu Staff Admin
   Fungsi : Tampilan Awal Staff Admin

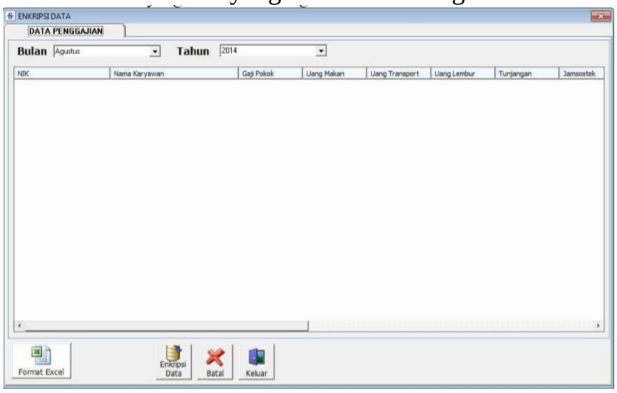
Gambar 14. Tampilan Menu Staff Admin

5. Nama Form : Menu *Tools*
   Fungsi : Tampilan Menu *Tools*



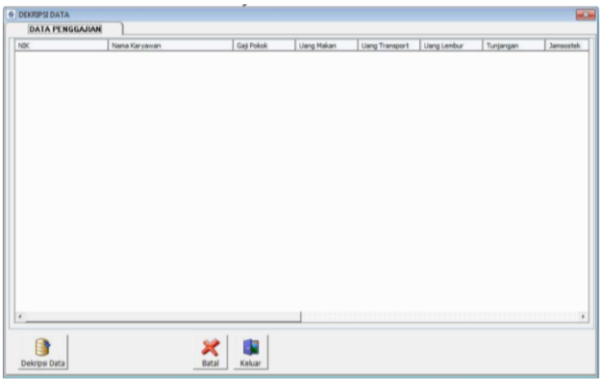
Gambar 15. Tampilan menu *Tools*

6. Nama Form : Form Enkripsi
   Fungsi : Untuk Mengenkripsi data penggajian agar tidak bisa dilihat oleh Pihak yang tidak berwenang.



Gambar 16. Form Enkripsi Data

7. Nama Form : Form Dekripsi
   Fungsi : Untuk Mendekripsi data yang sudah dienkripsi agar bisa dibaca dan dilihat isi datanya.



Gambar 17. Tampilan Form Dekripsi data

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan rumusan masalah dan pengamatan dilapangan mengenai proses berjalan pada PT. Sandipala Arthaputra maka penulis memiliki beberapa kesimpulan sebagai berikut :

1. Kesimpulan Terhadap Rumusan Masalah
   a. Tingkat keamanan data untuk penggajian di PT. Sandipala Arthaputra sangatlah rendah karena data penggajian diletakan dalam folder sharing dimana folder sharing tersebut bisa diakses dengan mudah.
   b. Terdapat Kendala dalam sistem yang saat ini sedang berjalan di PT. Sandipala Arthaputra. Berupa data yang berpotensi untuk dimanipulasi karena tidak ada otentikasi terhadap dokumen – dokumen penggajian..
   c. Perangkat Lunak *Authentication* dan *Digital Signature Scheme* dengan metode *Schnoor* akan sangat berpengaruh untuk mengatasi masalah keamanan data penggajian karena ada otentikasi terhadap data-data penggajian sehingga tidak mudah dimanipulasi oleh pihak-pihak yang tidak berwenang.
2. Kesimpulan Terhadap Tujuan dan Manfaat Penelitian
   a. Tujuan
      1. Penulis jadi mengetahui apa dan bagaimana sistem pengolahan data yang dilakukan oleh PT. Sandipala Arthaputra.
      2. Penulis Dapat mengetahui kendala dan solusi dari sistem berjalan yang dilakukan oleh PT. Sandipala Arthaputra.
      3. Penulis mampu merancang suatu Perangkat Lunak Authentication dan Digital Signature Scheme dengan metode Schnoor Untuk di impelementasi Pada Data Penggajian di PT. Sandipala Arthaputra.

   b. Manfaat

   Penulis berharap agar penulisan penelitian ini dapat memberikan kontribusi berbagai pihak antara lain :

   1. Bagi Penulis

      Penelitian ini merupakan implementasi dari teori yang telah didapatkan semasa perkuliahan di STMIK Bina Sarana Global, selain itu penulis juga mengembangkan wawasan dan pengetahuan tentang masalah-masalah yang berhubungan dengan keamanan data penggajian yang tidak didapatkan dibangku kuliah.
   2. Bagi Perusahaan

      Penelitian ini bisa dijadikan masukan yang dapat dikembangkan berkenaan dengan masalah yang dibahas untuk membantu kinerja PT. Sandipala Arthaputra dalam menjaga keamanan data Penggajian.
   3. Bagi Dunia Pendidikan

      Penelitian ini bisa digunakan sebagai tambahan informasi dan sumber bagi pihak yang berkompeten terhadap masalah yang dibahas, sekaligus sebagai bahan perbandingan dari laporan sejenis yang pernah dibuat sebelumnya dan juga diharapkan dapat memberikan kontribusi sebagai sumber ilmiah.
3. Kesimpulan Terhadap Metode Penelitian .
   a. Observasi

   Penulis Melakukan Observasi yaitu dengan cara mendatangi langsung ke PT.Sandipala Arthaputra dan melakukan pengamatan terhadap sistem keamanan data yang sudah berjalan dan melakukan pertanyaan terhadap user mengenai system keamanan data yang digunakan.

   b. Studi Pustaka

   Studi Pustaka yaitu pengumpulan data-data dengan cara mempelajari berbagai bentuk bahan-bahan tertulis seperti buku-buku penunjang kajian, majalah, catatan-catatan maupun referensi lain yang bersifat tertulis.

B. Saran

Adapun saran yang dapat diberikan sebagai bahan pertimbangan bagi PT. Sandipala Arthaputra, antara lain :

1. Melakukan pembelajaran atau pelatihan kepada bagian yang akan menggunakan aplikasi tersebut, agar mudah dalam pemakaian sehingga dapat menggunakannya secara maksimal dan mendapatkan informasi yang diinginkan.
2. Jika terdapat kekurangan pada sistem yang sedang diusulkan, hendaknya dicatat oleh user atau orang yang bersangkutan dengan sistem ini, hal ini ditunjukan untuk perbaikan sistem agar menjadi lebih sempurna.
3. Adapun data yang tersimpan dalam file komputer sangat penting, maka perlu dibuat file duplikat berupa print out. Guna menghindari kehilangan data ketika adanya gangguan pada sistem tersebut. Setelah menggunakan sistem tersebut, alangkah baiknya agar Perangkat Lunak *Authentication* dan *Digital Signature Scheme* dengan metode *Schnoor* tersebut dilakukan pengembangan agar lebih bermanfaat.

DAFTAR PUSTAKA

[1] J. M. Ecols dan H. Shadily, *Kamus Indonesia-Inggris*, Jakarta: PT Elex Media Komputindo, 2010.

[2] J. Kurniawan, *Kriptografi, Keamanan Internet dan Jaringan Komunikasi, Informatika*, Bandung, 2009.

[3] A. B. Ladjamuddin, *Analisis dan Desain Sistem Informasi*, Yogyakarta: Graha Ilmu, 2010.

[4] M. Manullang, dan Marihot M, *Manajemen Sumber Daya Manusia II*, Jakarta: Erlangga, 2012.

[5] R. Munir, *Kriptografi*, Bandung: Informatika, 2011.

[6] A. S. Nitisemito, *Majemen Personalia*, Edisi-3, Jakarta Timur: Penerbit Ghalia Indonesia, 2012.

[7] B. Nugroho, *Pemrograman Database SQL Server dengan Visual Basic 6.0*, Yogyakarta: Penerbit Gava Media, 2012.

[8] H. Purwono, *Sistem Personalia*, Edisi Ke-3, Yogyakarta: Andi Offset, 2009.

[9] B. Schneier, *Applied Crytography*, Second Edition, John Willey & Sons Inc., 2009.

[10] Swastha, dan Sukotjo, *Manajemen Personalia*, Edisi KE-5, BPFE-Yogyakarta 2010.